国内導入実績No.1のWAFでPCIDSS対策

～パスワードリスト攻撃やL7 DDoSの対策方法～

2015年7月28日

バラクーダネットワークスジャパン株式会社
セールスエンジニア
澤入　俊和

Barracuda

会社紹介

複雑なITをシンプルに

- 全てのお客様にシンプルなセキュリティとストレージ・ソリューションを提供します -

バラクーダネットワークス会社概要

バラクーダネットワークス　米国本社

2002年 Barracuda Networks, Inc.　設立

本社：カリフォルニア州キャンベル

海外拠点10カ国、80カ国以上で正規代理店と提携

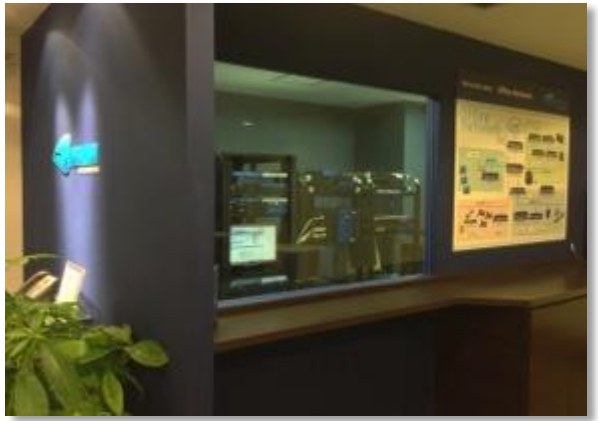
全世界15万社のお客様にセキュリティ・バックアップソリューションを提供

バラクーダバックアップは、バックアップ専用アプライアンスとしてシェアNo.1
(IDC Worldwide Quarterly Purpose Built Backup Appliance（PBBA）Tracker Q2/Q4)

2005年 バラクーダネットワークスジャパン株式会社 設立

スパムメール対策アプライアンスは2005年から2011年、7年間連続で国内出荷台数No.1。5,000台以上の出荷実績 （富士キメラ総研）

WAFも2007年から2013年まで7年連続国内No1の導入実績 （富士キメラ総研）



バラクーダネットワークス
ジャパンオフィス

2013年11月6日 Barracuda Networksは ニューヨーク証券取引所に上場しました

グローバル規模での
Barracuda Networksの取り組み

日本国内でのマーケティングの取り組み

9 種類の幅広い製品展開

仮想アプライアンス対応
マイナンバー対応製品
Microsoft Azure対応
Amazon AWS対応
vCloud Air対応

Barracuda Cloud Control

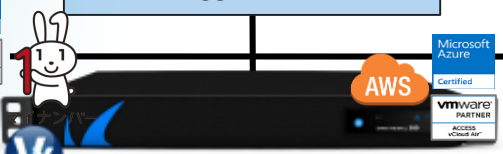
- 集中管理
- クラウドストレージ
- クラウドリレー

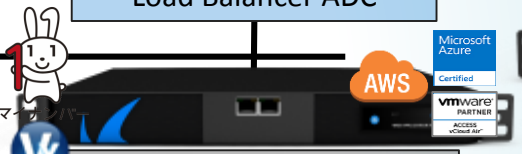
次世代ファイアウォール
NextG Firewall

リモートアクセス
SSL VPN

サーバ負荷分散/ADC
Load Balancer ADC

次世代ファイアウォール
Barracuda Firewall





アンチスパム/ウイルス
Spam Firewall Plus

Web脆弱性対策
Web Application Firewall

URLフィルタ・マルウェア対策
Web Filter

Webサーバ

TOTAL THREAT PROTECTION

DATA PROTECTION PLUS

メールアーカイブ
Message Archiver

メールサーバ

バックアップ
Backup

ファイルサーバ

DBサーバ

なぜIPSや統合型製品では不十分なのか？

2015年版情報セキュリティの10大脅威（IPA）

順位	タイトル
1	オンラインバンキングやクレジットカード情報の不正利用
2	内部不正による情報漏えい
3	標的型攻撃による諜報活動
4	ウェブサービスへの不正ログイン
5	ウェブサービスからの顧客情報の窃取
6	ハッカー集団によるサイバーテロ
7	ウェブサイトの改ざん
8	インターネット基盤技術の悪用
9	脆弱性公表に伴う攻撃の発生
10	悪意のあるスマートフォンアプリ

ウェブサイトへの脅威がいずれも上位！！

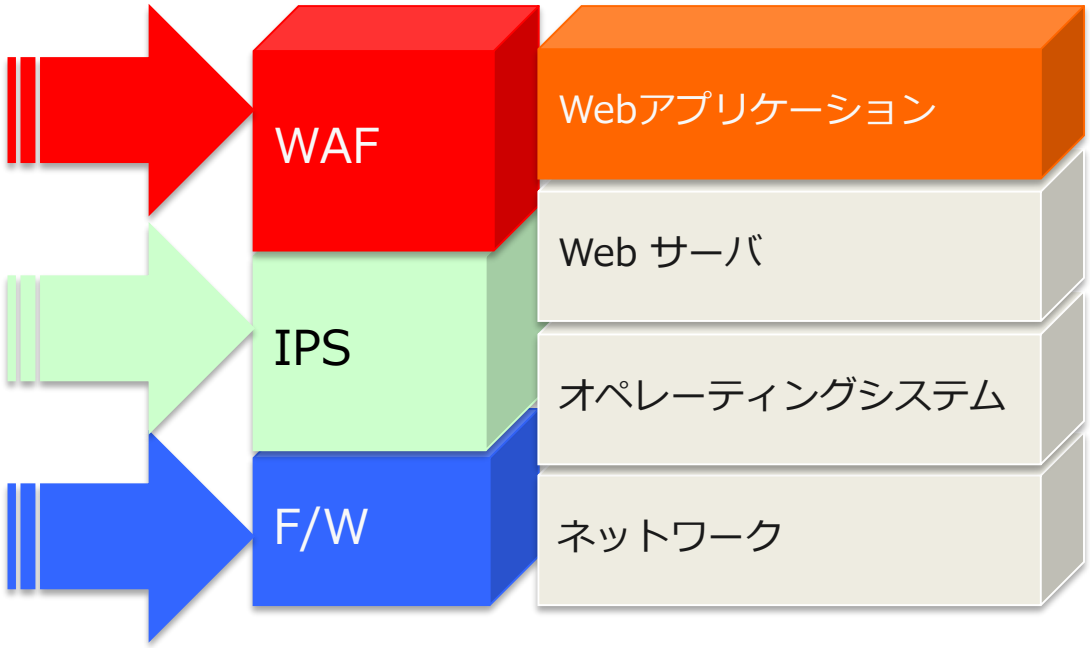
F/W、IPSとWAFは補完的関係

F/W、IPS、WAFはそれぞれ分野の異なるレイヤーの攻撃を防御する補完的関係
それぞれ、単体では、システムを完璧に実現することは出来ない

SQL・OSコマンドインジェクション
クロスサイトスクリプティング
Cookie・パラメータ改ざん
L7 DoS/DDoS

OS脆弱性対策
DoS/DDoS

ポートスキャン
IP/ポート制御



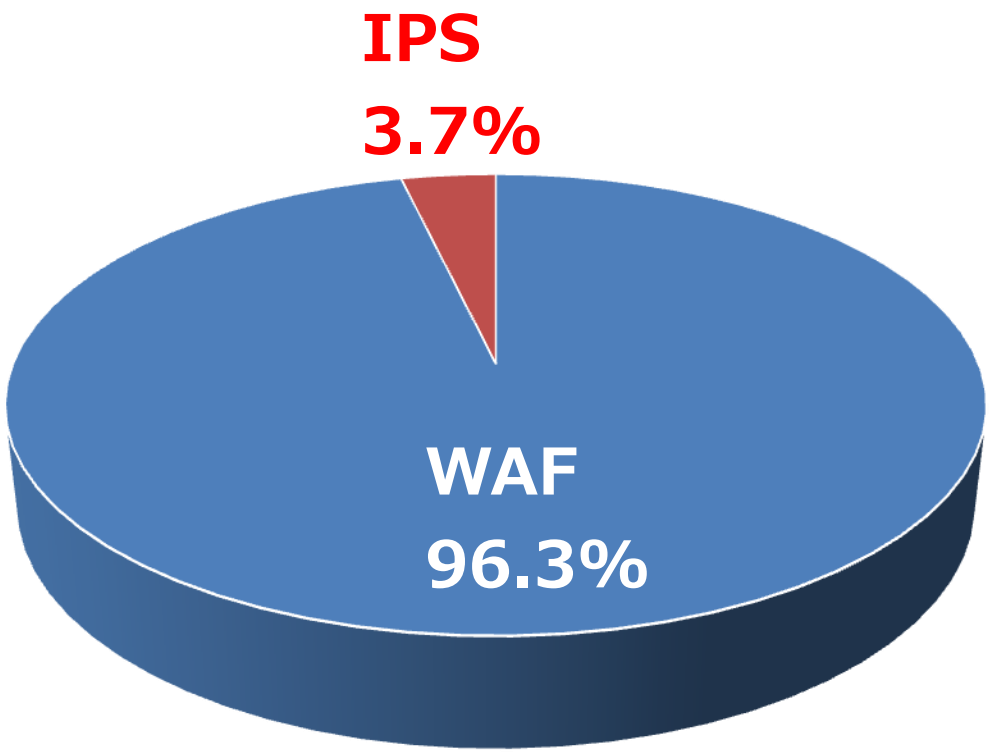
IPS/統合型製品で出来ること、出来ないこと

ウェブアプリへの主な攻撃	Barracuda WAF	IPS/統合型製品
SQLインジェクション	○	△*
OSコマンドインジェクション	○	△*
クロスサイトスクリプティング	○	△*
ディレクトリトラバーサル	○	△*
クロスサイトリクエストフォージェリー	○	×
強制ブラウズ	○	×
バッファオーバーフロー	○	×
パスワードリスト攻撃	○	×
パラメータ改ざん	○	×
クッキー改ざん	○	×
セッションハイジャック	○	×
スロークライアントアタック	○	×

・IPSでは攻撃が暗号化された場合検知不可、またはスループットが激減
・パスワードリスト攻撃など、最新の攻撃へ対応不可
・統合型製品もIPSと同様の機能しか搭載されていない

Webサイトへの攻撃の多くは上位レイヤーが対象

弊社検証サイトに対する攻撃数の内訳
(2015年2月18日-24日)



主な検知攻撃

- WAF
  SQLインジェクション
  エラーレスポンスの抑制
  ホストヘッダなし

- IPS
  バッファーオーバーフロー
  (CVE-2011-1567)
  Open SSL脆弱性

IPS防ぐことが出来る攻撃はごくわずか（3.7%)

最近のハッキング事件からみる
ウェブシステムへの攻撃手法

最近のハッキング事件からみる
ウェブシステムへの攻撃手法

第5位
ウェブサービスからの
顧客情報の窃取

大型 個人情報漏えい事件

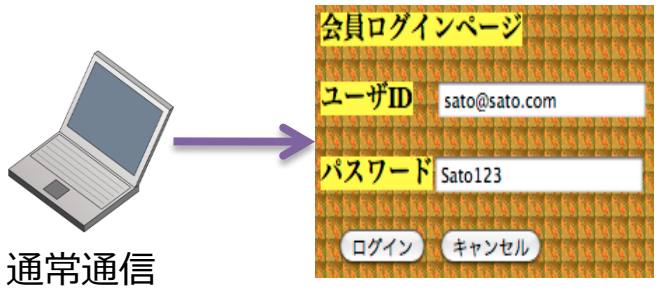
海外用データ通信機器レンタル会社

攻撃手法：SQLインジェクション

被害：10万9000件のカード情報、セキュリティコード、住所

SQLインジェクション攻撃

SELECT * FROM users WHERE uid=‘sato@sato.com' AND pwd=‘Sato123‘



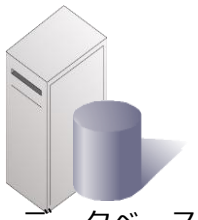
通常通信

正しいユーザIDと
パスワードであればログインが可能

Webアプリ

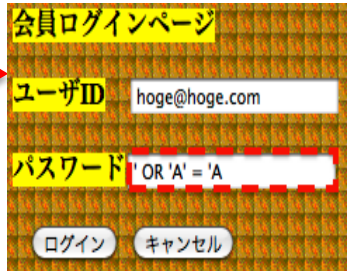
OK!

会員ページ表示



データベース

攻撃



ORの後は常に「真」の為
前の条件が全て打ち消される

SELECT * FROM users WHERE
uid=‘example@example.com' AND pwd=‘’OR 'A'='A‘

最近のハッキング事件からみる
ウェブシステムへの攻撃手法

第4位
Webサービスへの不正ログイン

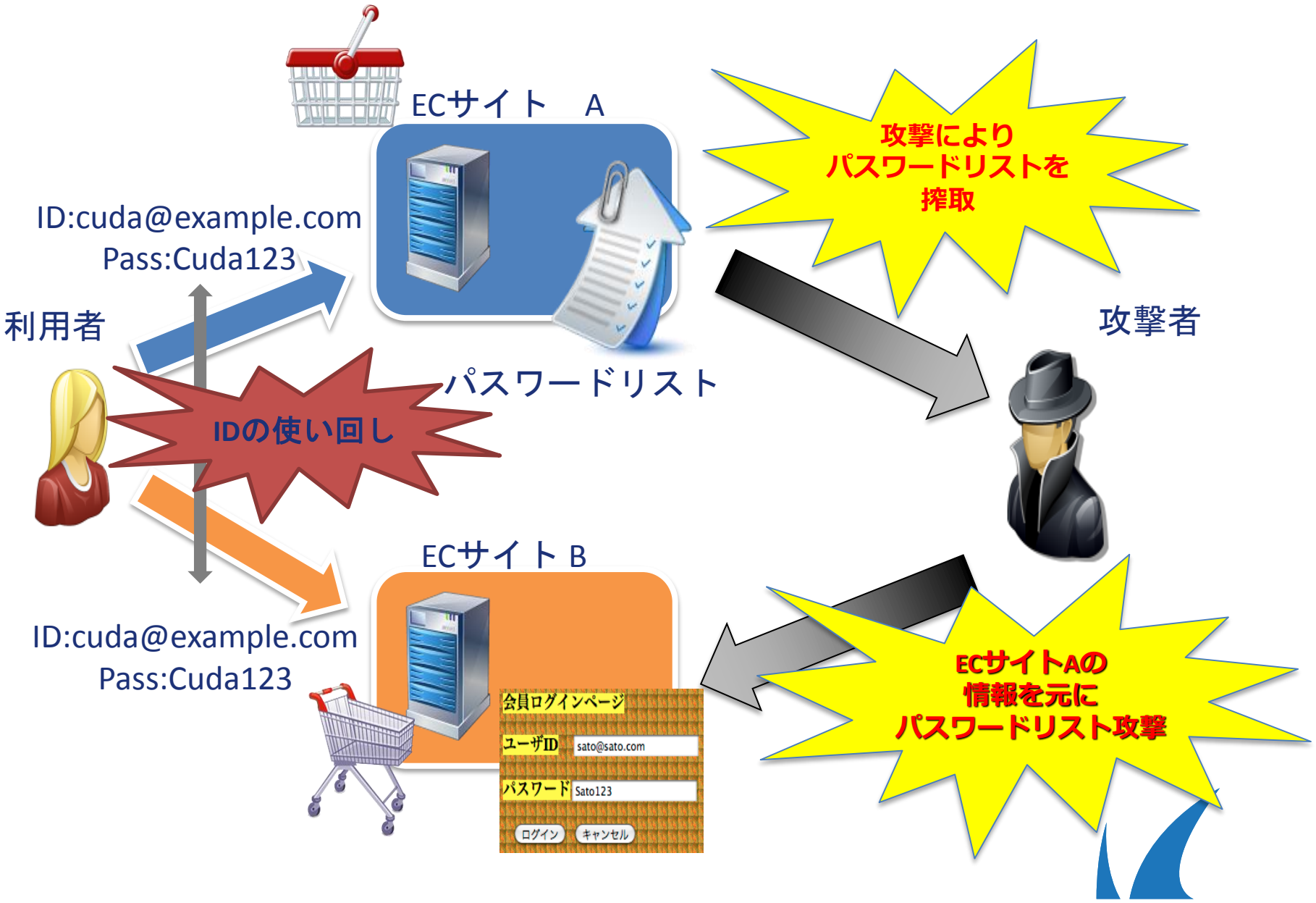
2014年 主な不正ログイン事件
（パスワードリスト攻撃）

		不正ログイン		
		試行	成功	**成功率**
6月	大手ブログサービス	2,293,543	38,280	**1.67%**
8月	大手小売業者　ＥＣサイト	4,220,382	20,957	**0.50%**
8月	大手電子マネーサービス	296,000	756	**0.26%**
9月	大手鉄道会社	11,520,000	21,000	**0.18%**
12月	リサーチ会社	3,161,872	1,320	**0.04%**

ブルートフォース攻撃に比べて、非常に効率的に不正ログインに成功

※一般的なブルートフォース攻撃の成功率　約0.001%

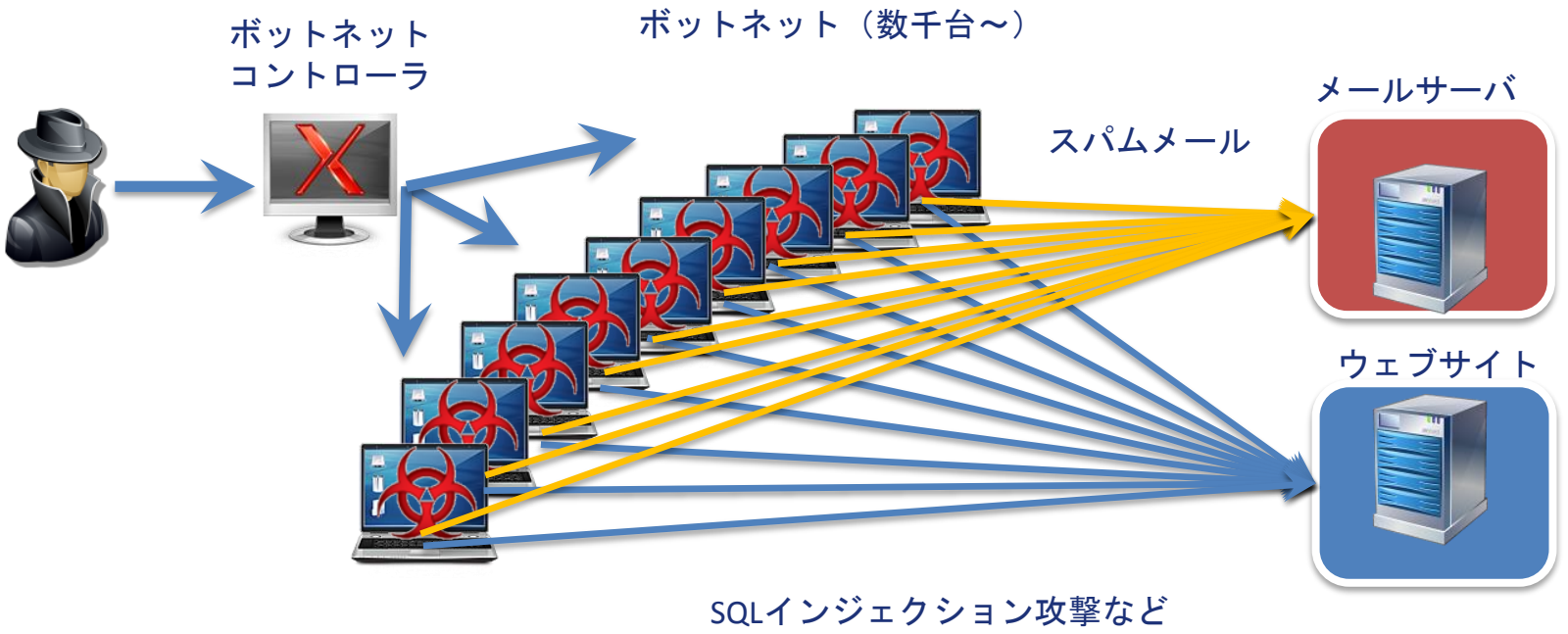
パスワードリスト攻撃の手口



最近のハッキング事件からみる
ウェブシステムへの攻撃手法

第6位
ハッカー集団による
サイバーテロ

ボットネットを利用するのはメールもウェブも同じ



L7 DDoS　Slow Client Attack

従来のSYN floodやSmurfなど、レイヤーの低い攻撃だけではなく、
最近のDDoS攻撃は、L7へ仕掛けてくるものが多数存在。

Slow HTTP Headers：ゆっくりリクエストヘッダを送り続ける。
Slow HTTP POST　　：ゆっくりPostデータを送信し続ける。
Slow Read DoS　　：レスポンスデータをゆっくりダウンロードする。

結果、サーバは大量のコネクションを保持し、ダウンする

ハッカーのメリット

- **ツールが存在しているため、非常に簡単**
- **サーバのコネクションタイムアウトを回避**
- **攻撃を検知されにくい**

```
GET / HTTP/1.1
Host: 172.16.xx.xx
User-Agent: Mozilla/4. (compatible;～～)
Content-Length: 42
X-a: b
X-a: b
X-a: b
X-a: b
 :
```

30秒から2分毎に1ヘッダ送る

Slow HTTP Headersの例

ネットワーク使用量の急増もなく、プロトコルとしては正しい通信のためFWやIPSでも検知できず、ISPでトラフィック量を監視していても検知できない

攻撃への対策

ハッキングの手口

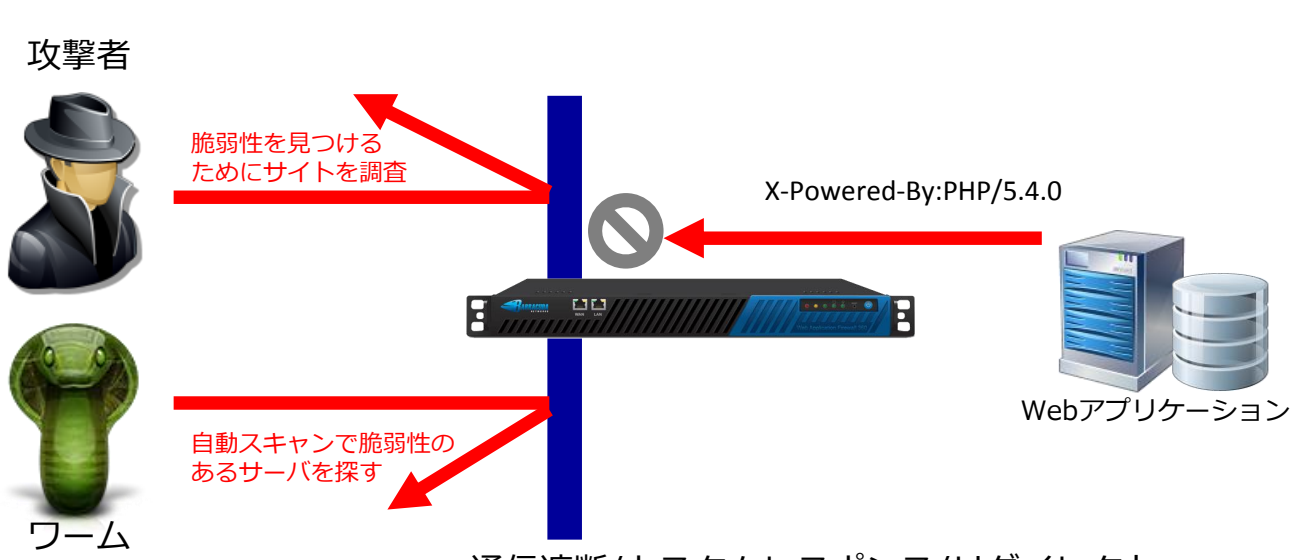
ウェブ攻撃は、
ほかの犯罪の手口と一緒

ターゲットを特定

防犯設備
分析・調査

弱点をつく

Webサイトクローキング



攻撃者がまず行うこと: 弱点を探すために、事前調査

- Webサーバ、データベースサーバ、アプリケーションサーバは、何を使用しているか？
- どんなバージョン、パッチを使用しているか？それらに、既知の脆弱性はあるか？

クローキングは、ハッカーやワームにWebリソースを隠す

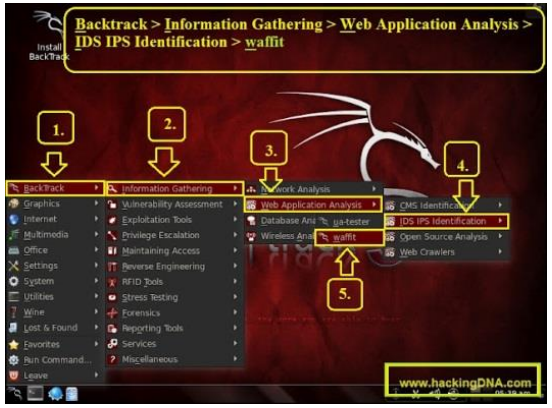
- エラーページ、エラーコード、HTTPヘッダー、IPアドレスを隠す

攻撃者に、攻撃される隙を与えない頑強なWebサイトに

情報収集対策

一般的なWAFは、改ざん防止のトラッキングのため、独自のCookieや、Hidden パラメータを挿入

WAFを使っているか、使っているなら、どんなWAFを使用しているかチェックするツールが存在




```
Checking http://
Generic Detection results:
No WAF detected by the generic detection
Number of requests: 9
```

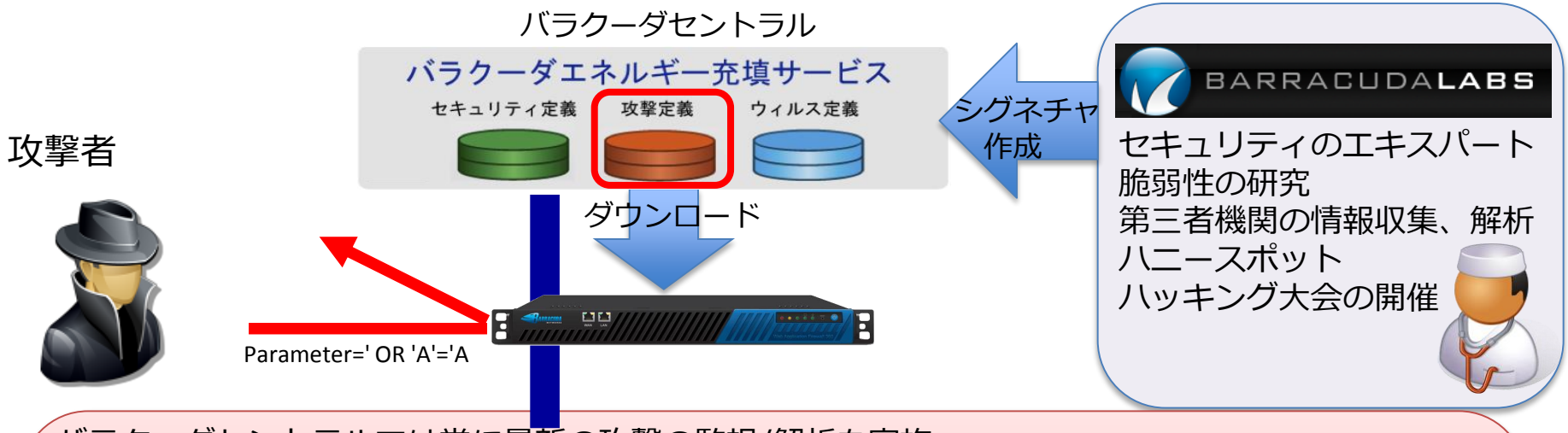
バラクーダのWAFは、Cookieやパラメータ名を変更可能！
判別される心配はありません。

攻撃への対策

SQLインジェクション

攻撃定義ファイルによる防御

難読化された攻撃も正規化を行ってシグネチャマッチングを実施



バラクーダセントラルでは常に最新の攻撃の監視/解析を実施
以下の攻撃をブロックすることが可能

- クロスサイトスクリプティング
- SQLインジェクション
- リモートファイルインクルージョン
- ディレクトリートラバーサル
- OSコマンドインジェクション

攻撃定義ファイルは常にバラクーダセントラルから最新のものをダウンロード
　更新間隔:10分から30分おきに更新
ブラックリスト型で簡単、最新の攻撃にもすぐに対応可能

※bash脆弱性、Shellshockへ対応済

WAFならサーバーを停止させることなく対応可能

攻撃への対策

パスワードリスト攻撃

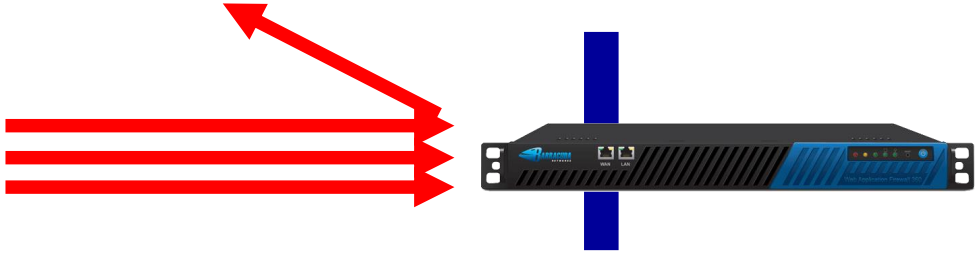
ブルートフォース攻撃＆パスワードリスト攻撃の防止

パスワード辞書総当たりによるログイン突破の攻撃

（**同一IP**がら同じようなり**リクエストを大量**に送りつける攻撃に有効）

攻撃者

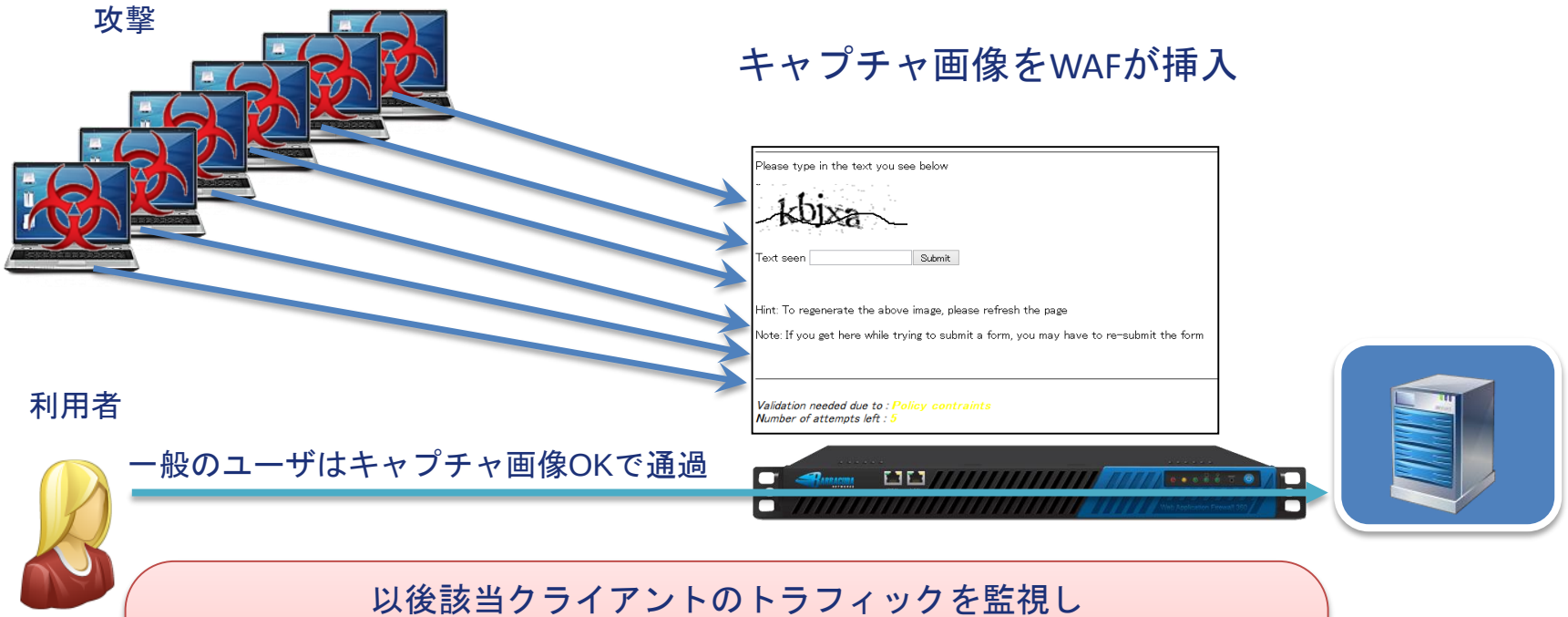
例）60秒以内に同一IPから
不正アクセスが10回あった場合
攻撃者とみなし防御



GET/POST数を監視、あらかじめ**設定した期間内**に、**同じIP**からの
リクエスト数をカウント。
決められた**閾値以上のアクセス**の際には**ブロック**する
（除外IPや特定URLのみ、認証エラーのみなど、柔軟に対応可能）

簡単な脆弱性を利用するスキャンツールを使ったハッカーの大部分をアクセス拒否
悪意のあるリクエストを防止することで正規のクライアントに適切なサービスを提供

ブロックしたくない場合、キャプチャ画像で緩和



以後該当クライアントのトラフィックを監視し
アイドル状態が継続すると再開時キャプチャ画像を表示

キャプチャが失敗すると通信拒否

パスワードリスト攻撃の緩和策としても有効

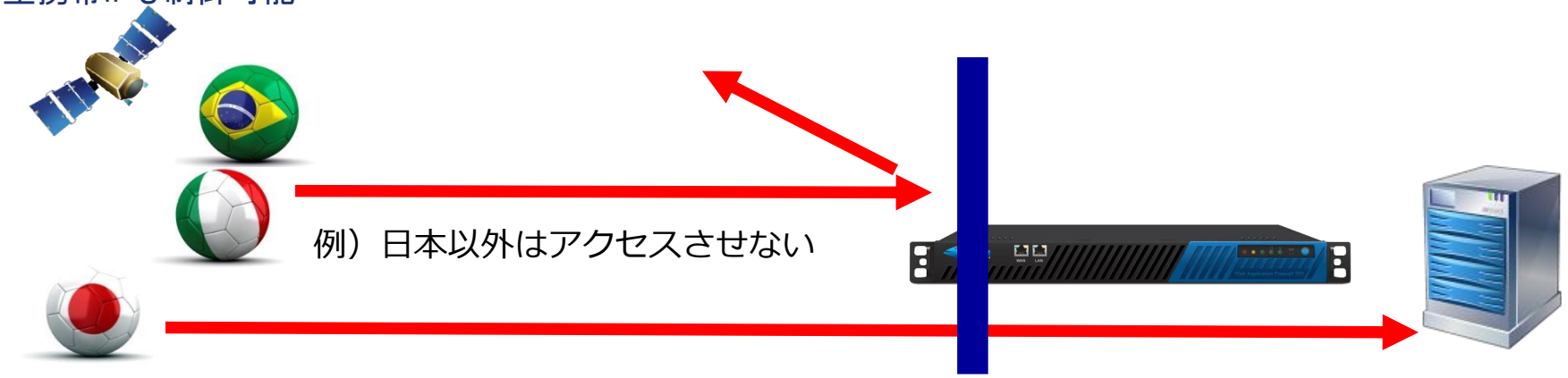
攻撃への対策

L7のDDoS攻撃

IPレピュテーション：国ごとに許可・拒否

国、地域IP辞書を搭載（自動更新）特定の国だけアクセス許可 or アクセス拒否

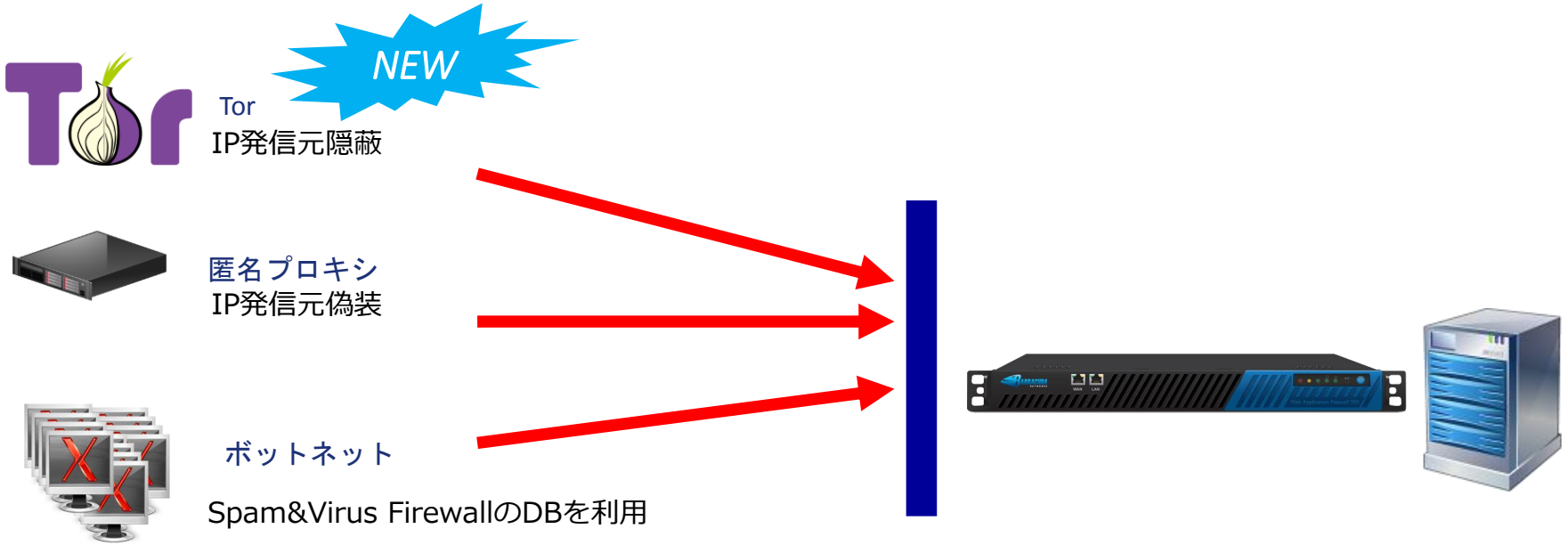
衛星携帯IPも制御可能



国情報、地域IP情報以外にも、衛星携帯電話を経由した通信の遮断も可能
IP情報は、定義ファイルによる自動更新のため、管理者が常にチェックする必要もありません。当然、例外設定も可能です。

サービス提供範囲が限定されている場合、危険にさらす頻度が少なくなり有効な手段

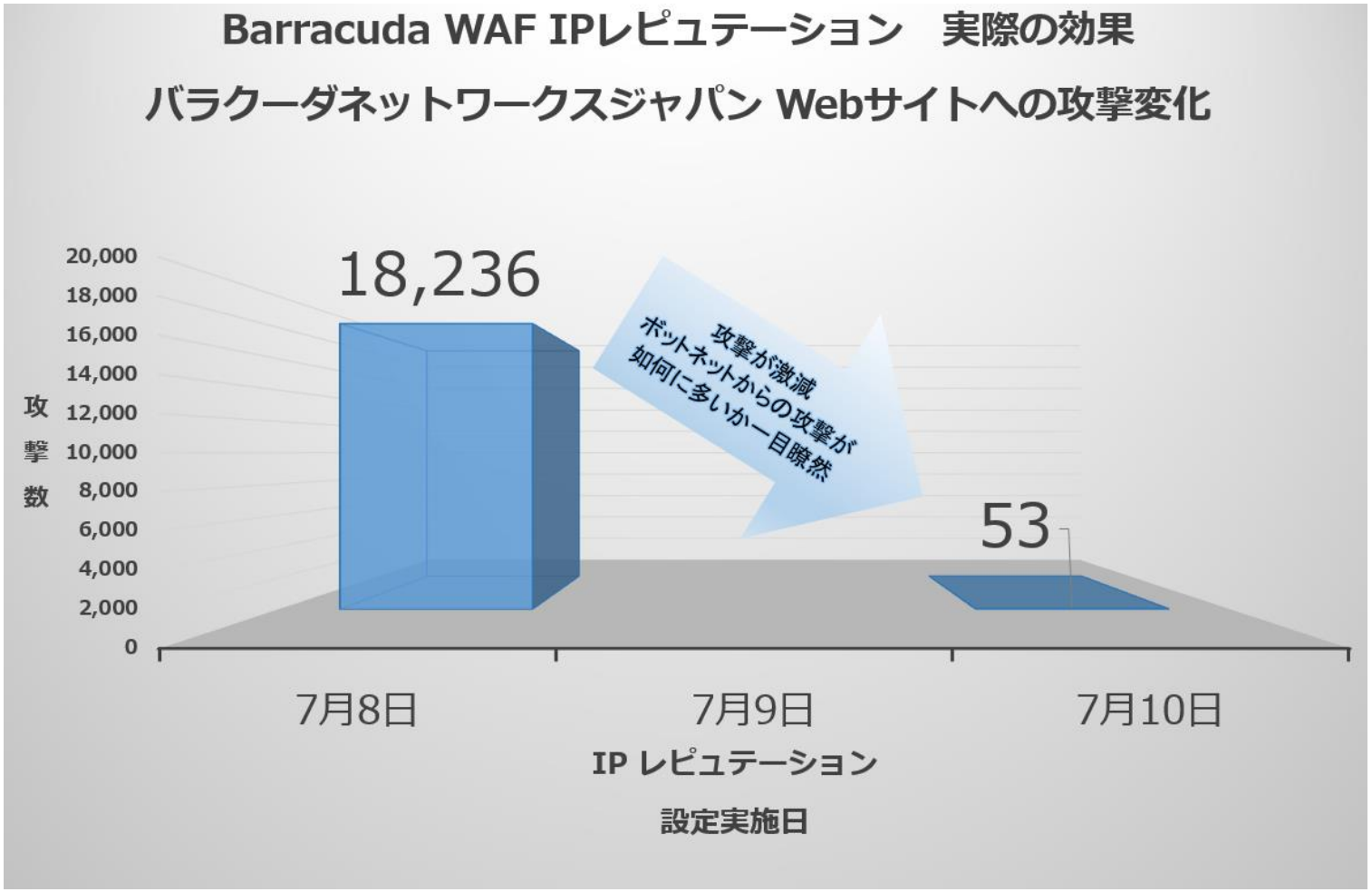
IPレピュテーション：疑わしいネットワークから通信拒否



・Torネットワーク（IP発信元隠蔽技術）***NEW!!***
・匿名プロキシ（Anonymous Proxy）
・ボットネットからのアクセス拒否
Spam＆Virus Firewall　Barracuda IP レピュテーションDBを利用
150,000台のBSVFからのボットネットの情報を活用
これらのIP情報も定義ファイルとして自動更新されます。

疑わしいしネットワークからのアクセスはお断り

ボットネットの通信遮断で、攻撃は、1/500へ激減

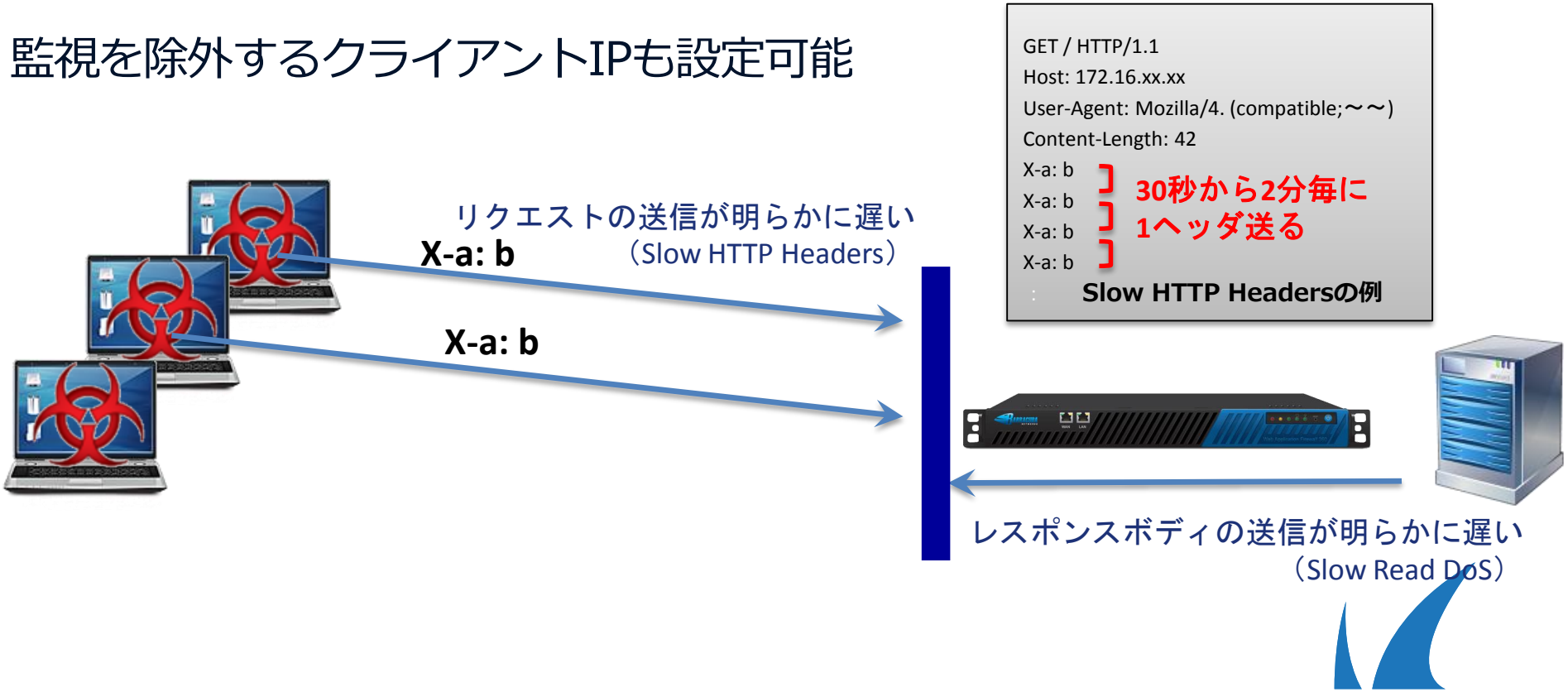


Slow Client 攻撃防御機能

通信量を常に監視して、単位時間当たりの
クライアント-WAF間の**平均通信量を計算**

想定した通信量よりも著しく少ない場合、
リアルタイムで攻撃と判断して、**WAFが通信を切断**

監視を除外するクライアントIPも設定可能



DDoS防御
～人間かロボットかを見分ける～

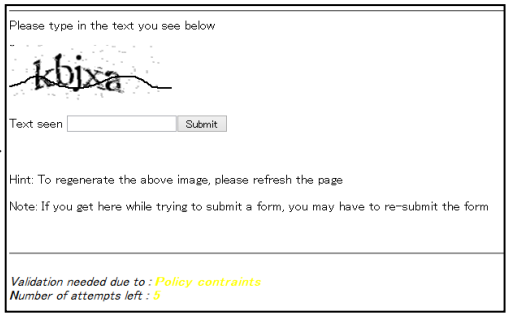
WAFが
JavaScript挿入

ブラウザの場合、
次のページのリクエスト時、JSの結果を
クッキーを送信

CudaCookie:12345678

クローラーやロボットの場合、
次のリクエスト時、JSの結果を判断できず
答えのクッキーを送信できない

失敗すると疑わしいと判断し
そのIPにキャプチャ画像を表示



PCI DSSとWAF

クレジットカードの不正利用被害は年々増加

PCI DSS 6.6 実装要件

一般公開されているWebアプリケーションで、継続的に新たな脅威や脆弱性に対処し、これらのアプリケーションが、**次のいずれかの方法**によって、既知の**攻撃から保護されていること**を確認する。

・一般公開されているWebアプリケーションは、アプリケーションのセキュリティ**脆弱性を手動/自動で評価するツール**または手法によって、少なくとも**年1回および何らかの変更を加えた後にレビュー**する

注：この評価は、要件11.2で実施する脆弱性スキャンとは異なる。

・Webベースの攻撃を検知および回避するために、一般公開されているWebアプリケーションの手前に、**Webアプリケーションファイアウォール**をインストールする。

PCI DSS 6.5 実装要件

PCIDSS要件	Barracuda製品での対応
6.5.1　インジェクションの不具合	○
6.5.2　バッファオーバーフロー	○
6.5.3　安全でない暗号化保存	○
6.5.4　安全でない通信	○
6.5.5　不適切なエラー処理	○
6.5.6　脆弱性特定プロセス	○
6.5.7　クロスサイトスクリプティング（XSS）	○
6.5.8　不適切なアクセス制御	○
6.5.9　クロスサイトリクエスト偽造（CSRF）	○

PCI DSS 3.0 主な変更点

・6.3：セキュアな開発ガイドラインを、内部ソフトウェアとカスタムソフトウェアの両方に適用

・6.5：よく発生するコーディングの脆弱性に関する開発者向けのトレーニングを更新し、機密性の高いデータをメモリで処理する方法を理解する

・6.5.10：認証の突破とセッション管理

・11.3：業界で認知されたアプローチをベースに侵入テストを実行する（NIST SP800-115など）

・11.3：侵入テストには、CDE境界と、ネットワーク内部／外部からのテストを含める。アプリケーションレイヤの侵入テストには、6.5（OWASP Top 10など）の要件を含める

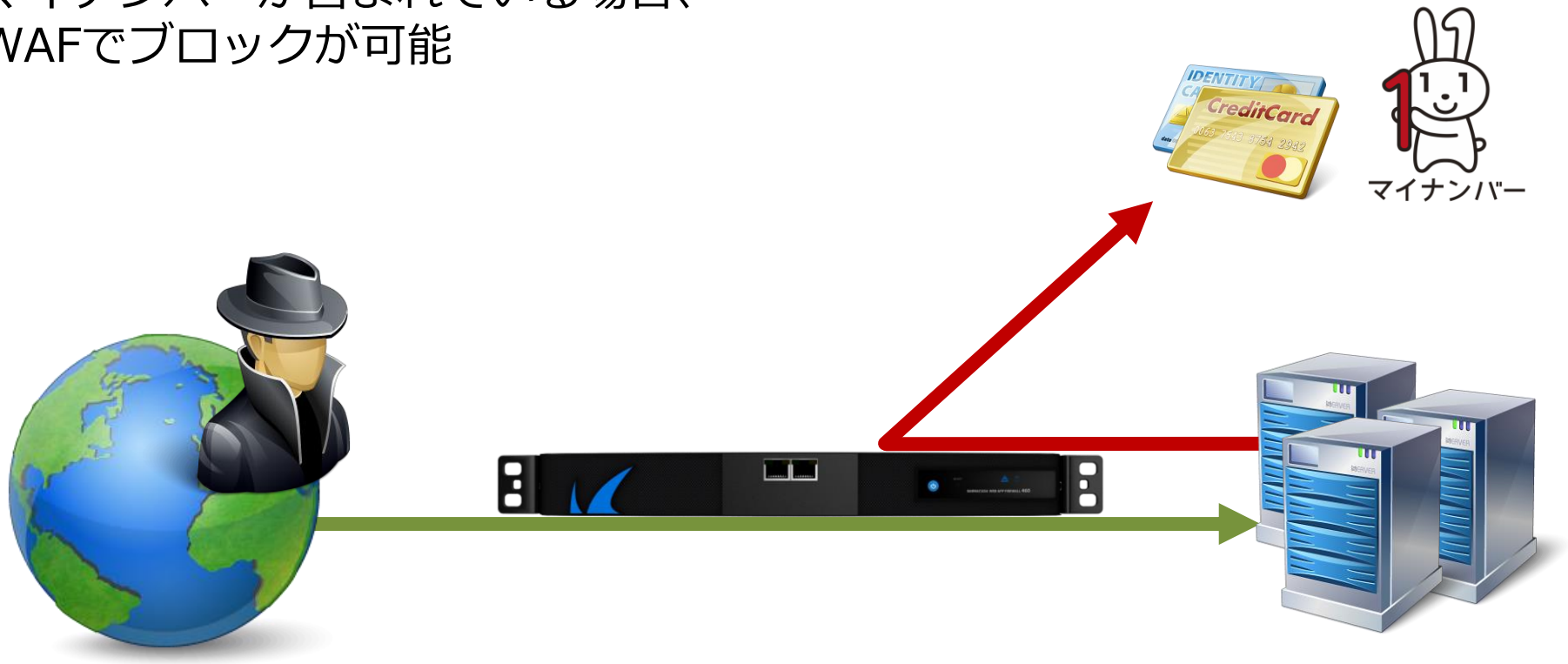
・11.3.1/11.3.2：年1回以上の内部／外部侵入テストに加え、インフラまたはアプリケーションの大幅なアップグレード／変更のたびに実施

・11.3.4：セグメンテーション制御および適用範囲の絞り込み制御を検証するテストを含める

要件6.6は大きな変更なし

データ盗難プロテクション機能

レスポンスにクレジットカード番号や
マイナンバーが含まれている場合、
WAFでブロックが可能

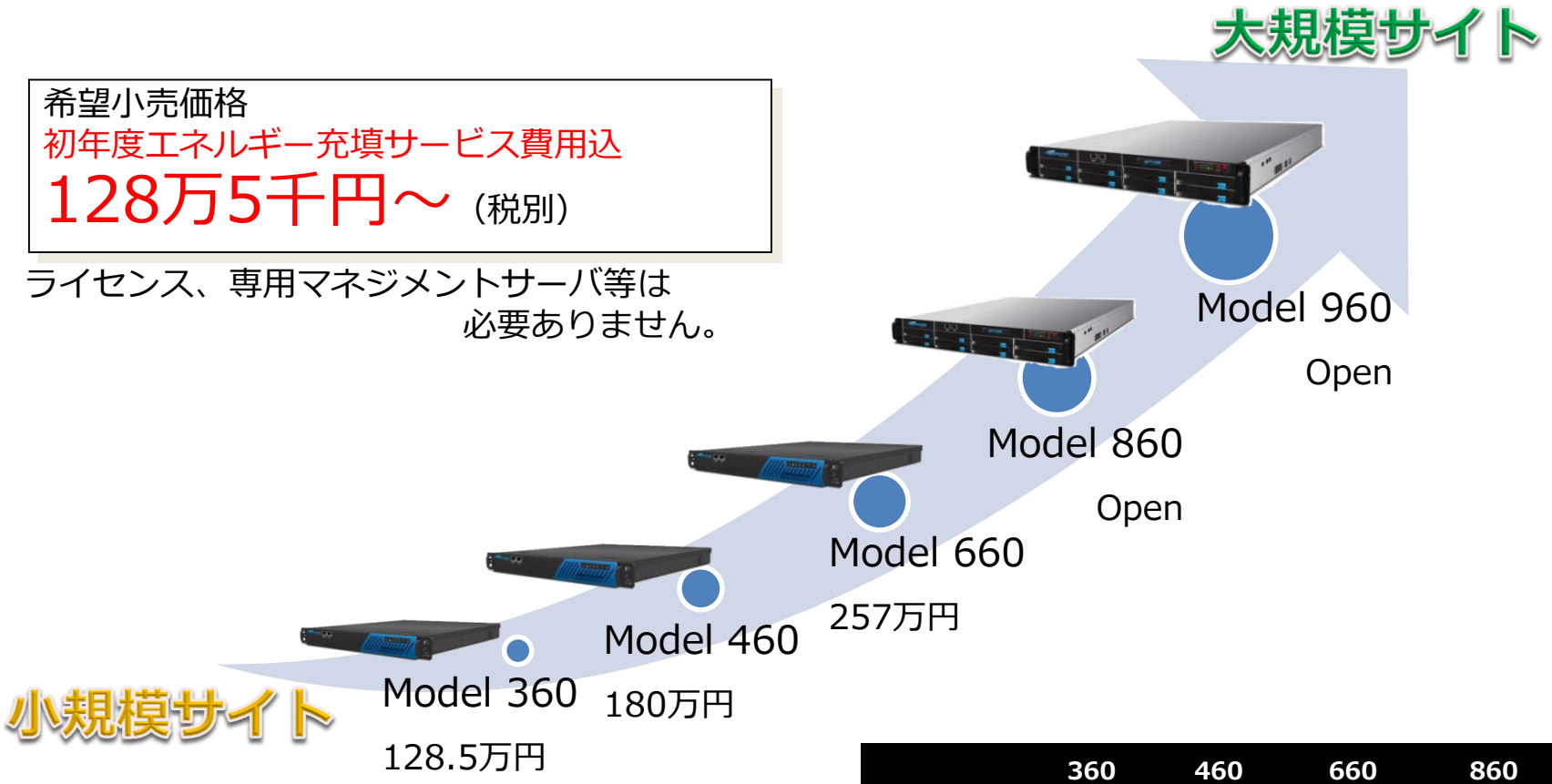


なぜ、Barracuda WAFなのか?

Barracuda Web Application Firewall シリーズ

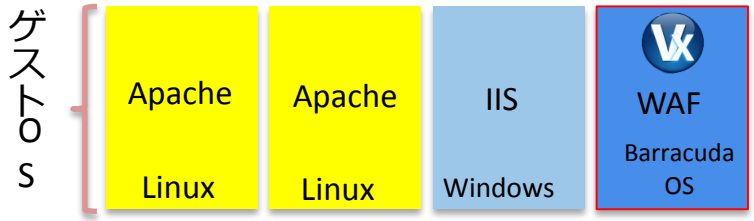
希望小売価格
初年度エネルギー充填サービス費用込
128万5千円～（税別）

ライセンス、専用マネジメントサーバ等は
必要ありません。



	360	460	660	860	960
実サーバ数	～5	～10	～25	～150	～300
スループット	25Mbps	50Mbps	200Mbps	1Gbps	4Gbps
秒間トランザクション（リクエスト数）					
HTTP	3,000	6,000	10,000	25,000	55,000
HTTPS	2,000	4,000	6,000	12,000	20,000

Barracuda Web Application Firewall
仮想アプライアンスシリーズ



対応するハイパーバイザ
VM ware ESX/ESXi
CITRIX XenServer
Microsoft Hyper-V

大規模サイト

小規模サイト

Model 360Vx

Model 460Vx

Model 660Vx

Model 660
+追加コアライセンス
最大計8コア 600Mbps

	360Vx	460Vx	660Vx
CPUコア数	2	3	4
目安スループット	25Mbps	50Mbps	100Mbps
秒間トランザクション（リクエスト数）			
HTTP	3,000	6,000	9,000
HTTPS	2,000	4,000	6,000

Windows Azure
Amazon AWSにも対応可能

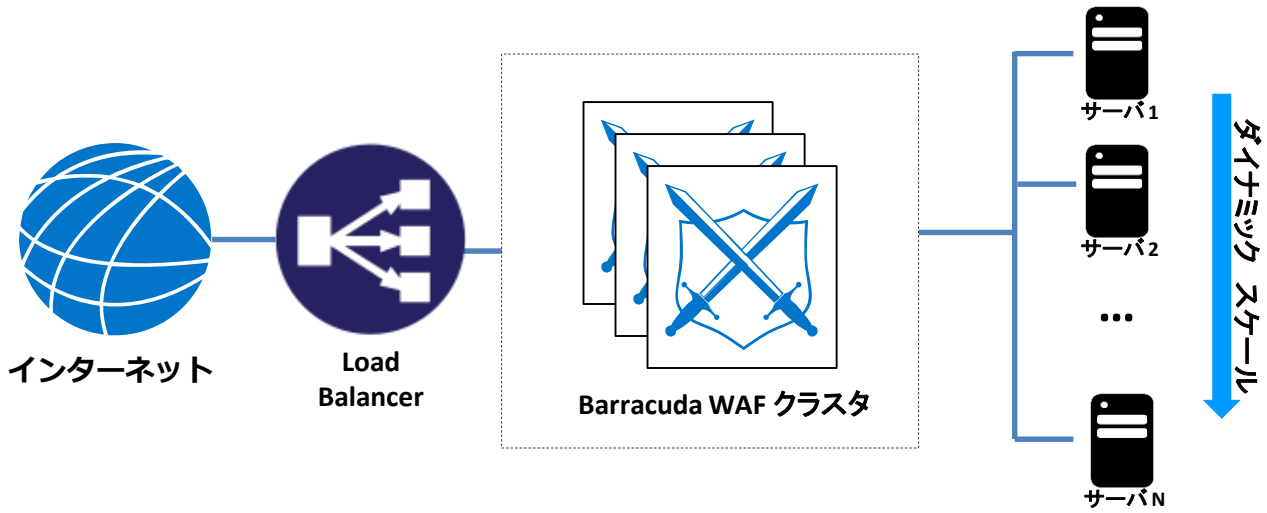
パブリッククラウドへの導入

Microsoft Azure

amazon web services™

New

vmware®



バラクーダネットワークスの最新情報をチェック

バラクーダネットワークス日本オフィシャルサイト
http://www.barracuda.co.jp/

バラクーダネットワークスジャパンFacebookページ
https://www.facebook.com/BarracudaNetworksJapan

バラクーダネットワークスTwitter
https://twitter.com/BarracudaJapan

YouTube Barracuda Japan チャンネル
https://www.youtube.com/user/BarracudaJapan

バラクーダネットワークスFoursquare
https://ja.foursquare.com/v/バラクーダネットワークスジャパン

バラクーダ製品を実際に試してみませんか？

- **無償貸出機**
  - 実際の環境でお試しいただけるよう、無償貸出機をご用意しております。
    - ご利用頂くには、貸出機がインターネットへアクセスできるようにFWの設定変更が必要です。
    - 一部製品では、プロキシはサポートしておりません。詳細はバラクーダネットワークスまでお問い合わせください
- **無償リモート検証環境（一部の製品で実施）**
  - FWの設定変更ができないお客様には簡易構成となりますが、弊社へリモートアクセス頂いてお試しいただけます。
- **ハンズオンセミナー・オンラインセミナー**
  - セミナーを随時開催しております。スケジュール等はバラクーダネットワークスまでお問い合わせください。

デモサイトをご活用ください

http://demo.barracuda.co.jp

全製品共通：
ユーザ名：**guest**
パスワード: **なし**

30日間
無償
評価機申込

GUIデモ

ありがとうございました

ご質問ございましたら、下記まで

より詳細な機能の説明
導入方法に関するご相談
30日間、評価機のご依頼（無料）　など

電話：03-5436-6235
メール：jpinfo@barracuda.com

バラクーダネットワークスジャパン株式会社

Barracuda